DOCKET NO.: 2013P109

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

SEUNG HYUN YOON, ET AL.

Application No.:

Filed:

For: **traffic measurement system and traffic analysis method thereof**

Art Group:

Examiner:

Commissioner for Patents
P.O, Box 1450
Alexandria, VA 22313-1450

REQUEST FOR PRIORITY

Sir:

Applicant respectfully requests a convention priority for the above-captioned application, namely:

COUNTRY	APPLICATION NUMBER	DATE OF FILING
Korea	2002-0079733	13 December 2002

☒ A certified copy of the document is being submitted herewith.

Respectfully submitted,

Blakely, Sokoloff, Taylor & Zafman LLP

Dated: 10/23/03

Eric S. Hyman, Reg. No. 30,139

12400 Wilshire Blvd., 7th Floor
Los Angeles, California 90025
Telephone: (310) 207-3800

KOREAN INTELLECTUAL PROPERTY OFFICE

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

Application Number:: Korean Patent Application 2002-0079733

Date of Application:: 13 December 2002

Applicant(s): : Electronics and Telecommunications Research Institute

30 December 2002

COMMISSIONER

[Bibliography]

[Document Name]	Patent Application
[Classification]	Patent
[Receiver]	Commissioner
[Reference No.]	0002
[Filing Date]	13 December2002
[IPC]	H04L
[Title]	Traffic measurement system and traffic analysis method thereof
[Applicant]	
[Name]	Electronics and Telecommunications Research Institute
[Applicant code]	3-1998-007763-8
[Attorney]	
[Name]	Youngpil Lee
[Attorney code]	9-1998-000334-6
[General Power of Attorney Registration No.]	2001-038378-6
[Attorney]	
[Name]	Haeyoung Lee
[Attorney code]	9-1999-000227-4
[General Power of Attorney Registration No.]	2001-038396-8
[Inventor]	
[Name]	YOON, Seung Hyun
[Resident Registration No.]	690131-1031413
[Zip Code]	305-804
[Address]	Rm. 203 ,146-14 Shinsung-dong, Yusong-gu Daejeon-city, Rep. of Korea
[Nationality]	Republic of Korea
[Inventor]	
[Name]	JEONG, Tae Soo
Resident Registration No.]	570923-1691716
[Zip Code]	305-755
[Address]	132-402 Hanbit Apt., Eoeun-dong, Yusong-gu, Daejeon-city Rep. of Korea
[Nationality]	Republic of Korea

[Inventor]
[Name] CHOI, Tae Sang
[Resident Registration No.] 620720-1690217
[Zip Code] 305-761
[Address] 106-707 Expo Apt. 464-1 Jeonmin-dong, Yusong-gu Daejeon-city, Rep. of Korea
[Nationality] Republic of Korea

[Inventor]
[Name] KIM, Hyung Hwan
[Resident Registration No.] 650920-1018441
[Zip Code] 305-729
[Address] 102-303 Cheonggunarae Apt., Jeonmin-dong, Yusong-gu Daejeon-city, Rep. of Korea
[Nationality] Republic of Korea

[Inventor]
[Name] CHUNG, Hyung Seok
[Resident Registration No.] 670209-1046414
[Zip Code] 305-751
[Address] 318-603 Songgang Green Apt., Songgang-dong, Yusong-gu Daejeon-city, Rep. of Korea
[Nationality] Republic of Korea

[Inventor]
[Name] PARK, Jeong Sook
[Resident Registration No.] 720202-2789912
[Zip Code] 305-804
[Address] 146-1 Shinsung-dong, Yusong-gu, Daejeon-city, Rep. of Korea
[Nationality] Republic of Korea

[Inventor]
[Name] KIM, Chang Hoon
[Resident Registration No.] 750327-1822318
[Zip Code] 305-804
[Address] Rm. 301 Greenvil 150-1 Shinsung-dong , Yusong-gu Daejeon-city, Rep. of Korea
[Nationality] Republic of Korea

[Request for Examination] Requested

[Purpose]	We file as above according to Art. 42 of the Patent Law request the examination as above according to Art. 60 of the Patent Law.	
	Attorney	Youngpil Lee
	Attorney	Haeyoung Lee

[Fee]		
[Basic page]	20 Sheet(s)	29,000 won
[Additional page]	2 Sheet(S)	2,000 won
[Priority claiming fee]	0 Case(S)	0 won
[Examination fee]	16 Claim(s)	621,000 won
[Total]	652,000 won	
[Reason for Reduction]	Government Invented Research Institution	
[Fee after Reduction]	326,000 won	

[Transfer of Technology]	
[Assignment of Technology]	Allowable
[Licensing]	Allowable
[Technology Training]	Allowable

[Enclosures]
1. Abstract and Specification (and Drawings) 1 copy

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0079733
Application Number PATENT-2002-0079733

출 원 년 월 일 : 2002년 12월 13일
Date of Application DEC 13, 2002

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Institu

2002 년 12 월 30 일

특 허 청 장
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0002
【제출일자】	2002.12.13
【국제특허분류】	H04L
【발명의 명칭】	트래픽 측정 시스템 및 그의 트래픽 분석 방법
【발명의 영문명칭】	Traffic measurement system and traffic analysis method thereof
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	2001-038378-6
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2001-038396-8
【발명자】	
【성명의 국문표기】	윤승현
【성명의 영문표기】	YOON,Seung Hyun
【주민등록번호】	690131-1031413
【우편번호】	305-804
【주소】	대전광역시 유성구 신성동 146-14 203호
【국적】	KR
【발명자】	
【성명의 국문표기】	정태수
【성명의 영문표기】	JEONG,Tae Soo
【주민등록번호】	570923-1691716

【우편번호】 305-755
【주소】 대전광역시 유성구 어은동 한빛아파트 132-402
【국적】 KR
【발명자】
【성명의 국문표기】 최태상
【성명의 영문표기】 CHOI,Tae Sang
【주민등록번호】 620720-1690217
【우편번호】 305-761
【주소】 대전광역시 유성구 전민동 464-1 엑스포아파트 106-707
【국적】 KR
【발명자】
【성명의 국문표기】 김형환
【성명의 영문표기】 KIM,Hyung Hwan
【주민등록번호】 650920-1018441
【우편번호】 305-729
【주소】 대전광역시 유성구 전민동 청구나래아파트 102동 303호
【국적】 KR
【발명자】
【성명의 국문표기】 정형석
【성명의 영문표기】 CHUNG,Hyung Seok
【주민등록번호】 670209-1046414
【우편번호】 305-751
【주소】 대전광역시 유성구 송강동 송강그린아파트 318-603
【국적】 KR
【발명자】
【성명의 국문표기】 박정숙
【성명의 영문표기】 PARK,Jeong Sook
【주민등록번호】 720202-2789912
【우편번호】 305-804
【주소】 대전광역시 유성구 신성동 146-1번지
【국적】 KR

【발명자】

【성명의 국문표기】	김창훈
【성명의 영문표기】	KIM,Chang Hoon
【주민등록번호】	750327-1822318
【우편번호】	305-804
【주소】	대전광역시 유성구 신성동 150-1 그린빌 301호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 이영필 (인) 대리인 이해영 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	2	면	2,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	16	항	621,000 원
【합계】	652,000 원		
【감면사유】	정부출연연구기관		
【감면후 수수료】	326,000 원		

【기술이전】

【기술양도】	희망
【실시권 허여】	희망
【기술지도】	희망
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

트래픽 측정 시스템 및 그의 트래픽 분석 방법이 개시된다. 본 발명에 따른 트래픽 측정 시스템은 인터넷 회선에 흐르는 모든 패킷을 수집하고, 수집된 패킷에서 트래픽 분석에 필요한 정보만을 추출하고, 추출된 정보를 소정의 플로우 형태로 가공하는 다수의 측정장치 및 다수의 측정장치들 각각에서 전달되는 트래픽 정보를 상호연계 분석하여 트래픽의 응용을 식별하고, 식별된 응용을 소정의 트래픽 유형으로 분류하여 그 결과를 출력하는 분석서버를 포함하는 것을 특징으로 하며, 인터넷망에서 트래픽을 측정하고 이를 가공하여 상세한 응용별 트래픽 통계자료를 생성할 수 있다. 특히, 다지점의 측정자료를 동시에 고려하여 분석하고, IP 패킷의 페이로드에 포함된 응용의 헤더로부터 응용을 식별할 수 있는 자료를 실시간으로 추출함으로써 상세한 트래픽 분석결과를 제공할 수 있다.

【대표도】

도 1

【명세서】

【발명의 명칭】

트래픽 측정 시스템 및 그의 트래픽 분석 방법{Traffic measurement system and traffic analysis method thereof}

【도면의 간단한 설명】

도 1은 본 발명에 따른 트래픽 측정 시스템의 일실시예를 나타내는 블록도이다.

도 2는 도 1에 도시된 트래픽 분석부(200)에서 트래픽 분석에 사용되는 트래픽 분류 유형의 일예를 나타내는 도면이다.

도 3은 도 1에 도시된 분석서버(20)에서 수행되는 트래픽 측정 및 분석 방법의 일실시예를 나타내는 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<4> 본 발명은 인터넷 망 측정 시스템에 관한 것으로, 특히, 여러 지점의 인터넷 회선에서 트래픽정보를 수집하고 이를 응용별로 상세히 분류하고 분석하는 트래픽 측정 시스템 및 그의 트래픽 분석 방법에 관한 것이다.

<5> 인터넷은 네트워크 구성 및 트래픽(traffic) 특성이 복잡하여 망을 측정하는 방법이 다양하게 제안되어 사용되고 있다. 트래픽 측정은 네트워크 초기단계의 설계 및 계획, 운영단계의 트래픽 엔지니어링 및 향후 고품질 인터넷서비스의 제공과 직접적으로

관계를 갖고 있으며, 모든 네트워크 관련작업에 있어서 기본적으로 수행해야 하는 작업이다.

<6> 네트워크 성능 측정 방법은 그 특성에 따라 능동 측정 방법과 수동 측정 방법으로 크게 나눌 수 있다. 능동 측정 방법은 시험 패킷을 네트워크에 부과하고, 패킷이 네트워크를 통과한 후 나타나는 지연, 손실 등의 특성을 측정하여 주로 망의 성능을 분석하는 방법이다. 수동 측정 방법은 네트워크 흐름에 영향을 주지 않으면서 현재 네트워크에 흐르는 패킷을 감시하고, 수집된 정보를 바탕으로 주로 트래픽 규모나 트래픽 구성 또는 특성 등을 분석하는 방법이다.

<7> 지금까지 트래픽 규모의 측정작업은 주로 장치내의 MIB(Management Information Base) 정보를 이용하여 각 회선의 사용율을 측정하는 방식을 사용해 왔다. 이러한 방법은 현재 장비기능이나 표준화 작업이 잘 되어 있기 때문에 쉽게 사용이 가능하지만 회선을 차지하는 트래픽의 규모를 얻는 것만을 목적으로 하고 있다. 따라서, 이를 이용하여 회선을 점유하는 트래픽의 구성 및 특성을 분석하는 것은 불가능하다. 이를 부분적으로 보완하기 위해서 통상 라우터에는 간단히 포트번호를 이용한 트래픽 분류기능이 있으나 과거에 비하여 매우 다양한 응용이 존재하는 현재 인터넷의 트래픽 특성을 나타내기는 거의 불가능하다.

<8> 현재 트래픽을 상세히 분석하기 위해서는 회선에서 패킷을 수집하거나 시스코의 넷플로우 기능 등을 이용하여 트래픽 정보를 수집한 후 사후분석을 수행하는 방법이 많이 사용된다. 이는 주로 연구목적으로 사용되거나 일시적으로 트래픽을 분석하기 위해 많이 사용되는 방법이다. 그러나 이러한 방법은 사후분석을 수행하

기 때문에 패킷정보를 보관해야 하고, 따라서 사용자 데이터와 관련될 가능성이 있는 패킷의 페이로드(Payload) 정보 등을 수집할 수 없는 경우가 대부분이다. 따라서, 응용에 관련된 정보들이 유실되어 IP/TCP/UDP 헤더 정보에 의지하여 분석을 수행할 수밖에 없다는 문제가 있다. 이와 같은 경우에 응용을 분류하기 위해서 사용될 수 있는 정보가 포트 번호에 국한되기 때문에 P2P나 스트리밍 서비스와 같이 전통적인 방법으로 포트를 사용하지 않는 응용에 대해서는 응용의 식별이 매우 어렵게 된다. 또한 정형화된 분석방법이 정립되어 있지 않기 때문에 근본적으로 많은 전문인력을 필요로 하며, 대용량의 저장장치나 고속의 서버장비를 갖추어야 한다. 결국, 연속적으로 장시간 측정 및 분석에 적용하기는 어렵다.

<9> 특히, 인터넷은 트래픽 경로가 비대칭이기 때문에 네트워크가 외부와 여러 회선으로 연결된 경우에 다지점에서 수집된 트래픽을 동시에 고려한 상호연계 분석이 이루어져야 하나 이를 위한 정형화된 시스템이나 방법이 아직까지 제시된 바 없다.

【발명이 이루고자 하는 기술적 과제】

<10> 본 발명이 이루고자 하는 기술적 과제는 다지점에서 트래픽을 측정하고, 측정된 다지점의 트래픽을 연계 분석함으로써, 상세한 트래픽 분석결과를 제공할 수 있는 트래픽 측정 시스템을 제공하는 데 있다.

<11> 본 발명이 이루고자 하는 다른 기술적 과제는 상기 트래픽 측정 시스템에서 수행되는 트래픽 분석 방법을 제공하는 데 있다.

<12> 본 발명이 이루고자 하는 또 다른 기술적 과제는 상기 트래픽 분석 방법을 컴퓨터에서 실행 가능한 프로그램 코드로 기록된 기록 매체를 제공하는 데 있다.

【발명의 구성 및 작용】

<13> 상기 과제를 이루기 위해, 본 발명에 따른 트래픽 측정 시스템은 인터넷 회선에 흐르는 모든 패킷을 수집하고, 수집된 패킷에서 트래픽 분석에 필요한 정보만을 추출하고, 추출된 정보를 소정의 플로우 형태로 가공하는 다수의 측정장치 및 다수의 측정장치들 각각에서 전달되는 트래픽 정보를 상호연계 분석하여 트래픽의 응용을 식별하고, 식별된 응용을 소정의 트래픽 유형으로 분류하여 그 결과를 출력하는 분석서버를 포함하는 것이 바람직하다.

<14> 상기 다른 과제를 이루기 위해, 인터넷 회선에 흐르는 패킷을 수집하여 트래픽 분석하여 패킷의 응용을 식별하는 트래픽 측정 시스템에서 수행되는 본 발명에 따른 트래픽 분석방법은 소정의 형태로 가공된 플로우 정보로부터 포트 번호만으로 응용식별이 가능한 제1트래픽 유형을 분류하는 (a)단계, 제1트래픽 유형을 식별하고 남은 플로우 정보에서 패킷의 페이로드에 포함된 응용헤더 및 동작관련 정보를 수집해야 응용식별이 가능한 제2트래픽 유형을 분류하는 (b)단계, 제2트래픽 유형을 식별하고 남은 플로우 정보와 다른 지점에서 측정된 해당 플로우의 역방향 플로우 정보를 상호 연계 분석함으로써 응용식별되는 제3트래픽 유형을 분류하는 (c)단계, 제3트래픽 유형을 식별하고 남은 플로우 정보중 포트번호가 정해져 있지 않아, 다른 지점에서 측정된 플로우 정보를 통하여 응용식별이 가능한 제4트래픽 유형을 분류하는 (d)단계 및 제4트래픽 유형을 식별하고 남은 플로우 정보를 제5트래픽 유형으로 분류하는 (e)단계를 포함하는 것이 바람직하다.

<15> 이하, 본 발명에 따른 트래픽 측정 시스템 및 그의 트래픽 분석 방법을 첨부한 도면들을 참조하여 다음과 같이 설명한다.

<16> 도 1은 본 발명에 따른 트래픽 측정 시스템의 일실시예를 나타내는 블록도이다. 본 발명에 따른 트래픽 측정 시스템은 측정장치들(10), 분석서버(20) 및 시각수신장치들(40)을 포함하여 구성된다. 도 1에는 설명의 편의를 위해 라우터들(30)이 함께 도시된다.

<17> 도 1을 참조하여, 시각수신장치들(40) 각각은 GPS 위성 또는 CDMA 기지국으로부터 시각신호를 추출하여 모든 측정장치들(10)의 시각이 동일하게 유지되도록 제어한다.

<18> 측정장치(10)는 인터넷 회선에 흐르는 모든 패킷을 수집하고, 수집된 패킷에서 트래픽 분석에 필요한 정보만을 추출 및 가공하여 분석 서버(20)로 제공한다. 바람직하게는, 측정장치(10)는 패킷 수집부(100), 플로우 생성부(110), 저장부(120) 및 전송부(130)를 포함하여 구성된다.

<19> 패킷 수집부(100)는 라우터간 연결회선으로부터 태핑, 포트 미러링 또는 신호 분배기 등을 사용하여 인터넷 회선에 흐르는 모든 패킷정보를 수집하고 각 패킷별로 시각수신장치(40)로부터 받은 정확한 시각을 기록하여 플로우 생성부(110)로 제공한다.

<20> 플로우 생성부(110)는 패킷 수집부(100)에서 수집된 패킷으로부터 동일한 주소, 동일한 프로토콜, 동일한 포트번호 등을 보유한 패킷을 하나의 플로우로 생성한다. 또한, 플로우 생성부(110)는 각 패킷의 내용을 분석하여 응용(application)별 상세 분석에 필요한 정보 즉, 패킷의 페이로드(payload)에서 응용을 판단할 수 있는 동작관련 정보를 추출하며, 추출된 정보는 저장부(120)에 임시 저장한다.

<21> 전송부(130)는 정해진 시간에 따라 저장부(120)에 저장된 정보를 분석서버(20)에 전송한다.

<22> 계속해서, 분석서버(20)는 다수의 측정장치들(10) 각각에서 전달되는 정보를 상호 연계 분석하여 트래픽을 응용별로 상세히 분류하고 각각에 대한 트래픽 통계를 산출하여 회선에 대한 트래픽 보고서를 생성한다. 바람직하게는, 분석서버(20)는 트래픽 분석부(200), 데이터 수신부(210), 보고서 출력부(220), 자료 저장부(230) 및 사용자 인터페이스(240)를 포함하여 구성된다.

<23> 데이터 수신부(210)는 다수의 측정장치들(10)로부터 전송되는 수집된 정보를 수신하여 트래픽 분석부(200)로 제공한다.

<24> 트래픽 분석부(200)는 데이터 수신부(210)로부터 제공받은 정보를 상호 연계하여 응용별 상세 분석하고, 분석 결과를 자료 저장부(230)에 저장하거나 보고서 출력부(220)로 제공한다.

<25> 보고서 출력부(220)는 트래픽 분석부(200)에서 분석된 자료를 소정의 보고서 형태로 가공하여 자료 저장부(230)에 저장한다.

<26> 사용자 인터페이스(240)는 자료 저장부(230)에 저장된 보고서 및 각종 분석자료를 사용자가 요구하는 다양한 방식으로 사용자에게 표시한다.

<27> 도 2는 도 1에 도시된 트래픽 분석부(200)에서 트래픽 분석에 사용되는 트래픽 분류 유형의 일예를 나타내는 도면이다.

<28> 도 2에 도시된 바와 같이, 본 발명에서는 트래픽을 총 5개의 유형으로 분류한다. 구체적으로, 본 발명에 따른 트래픽 유형은 TCP/UDP 포트번호만으로 분류되는 제1트래픽 유형(21), 패킷의 페이로드에 포함된 응용헤더 및 정보를 수집해야 식별되는 제2트래픽 유형(22), 제2트래픽 유형(22)의 역방향 트래픽 중에 자체적으로 응용에 관한 정보가 존

재하지 않기 때문에 제2트래픽 유형(22)로부터 정보를 추출해야만 식별이 가능한 제3트래픽 유형(23), 포트번호가 정해져 있지 않고 다른 플로우를 통하여 사용할 포트번호가 교환되기 때문에 다른 플로우의 내부정보를 바탕으로 식별해야 하는 제4트래픽 유형(24), 이상의 제1트래픽 유형(21) 내지 제4트래픽 유형(24) 중 어느 하나로도 분류되지 않는 제5트래픽 유형(25)로 나뉘어 분석된다.

<29> 도 2를 참조하여, 제1트래픽 유형(21)은 TCP/UDP에서 사용하는 포트번호에 있어서 특정한 포트를 하나의 응용만 사용하는 경우에 적용이 가능하다. 이러한 제1트래픽 유형(21)의 식별방법은 상대적으로 가장 간단한 것으로 기존에 트래픽을 분류할 때 많이 사용해 오던 방식이다. 현재 인터넷을 사용하는 응용 중 일부는 이에 해당될 수 있기 때문에 제1트래픽 유형(21)을 트래픽 분류 유형 중 하나로 정의한다.

<30> 제2트래픽 유형(22)는 하나의 포트번호를 여러 개의 응용이 같이 사용하는 경우에 해당되는 트래픽이다. 제2트래픽 유형(22)에 해당되는 트래픽의 경우는 포트번호만으로 응용을 식별할 수 없으며, IP/TCP/UDP 헤더이외에 패킷의 페이로드 중 응용에 관련된 헤더나 식별기호 등을 활용해야만 트래픽을 분류할 수 있다. 특히, 포트번호가 1024 이상인 것들은 서버-단말로 구성된 프로그램에 있어서 항상 단말측 포트번호로 임의로 사용될 수 있다. 즉, 포트번호를 1024 이상으로 할당하여 만들어진 응용의 경우는 항시 해당 포트번호를 다른 응용이 사용하는 것과 중복이 일어날 수 있다. 따라서, 이러한 경우 IP/TCP/UDP 헤더이외에 패킷의 페이로드 중 응용에 관련된 헤더나 식별기호 등을 이용하여 트래픽을 분류해야 한다.

<31> 제3트래픽 유형(23)은 제2트래픽 유형(22)에 해당되는 포트번호를 사용하되 이를 식별할 수 있는 응용헤더나 식별기호 등이 해당 플로우에 포함되어 있지 않은 트래픽이

다. 이를 분석하기 위해서는 같은 회선 또는 다른 회선에 나타날 수 있는 제3트래픽 유형(23)의 역방향 트래픽인 제2트래픽 유형(22)으로부터 응용을 식별하는 정보를 추출해야 한다. 특히, 인터넷은 트래픽 경로가 비대칭이기 때문에 순방향 플로우와 역방향 플로우가 같은 회선에 나타나지 않는 경우가 많다. 따라서 이러한 제3트래픽 유형(23)의 식별가능성을 높이기 위해서는 다수의 측정 장치들(10)에서 측정된 결과를 상호 연계하여 분석하는 것이 바람직하다.

<32> 제4트래픽 유형(24)는 스트리밍 서비스 응용에서 많이 나타나는데, 이러한 응용들은 서버-단말간 서비스를 위해서 2개 이상의 TCP 또는 UDP 연결을 사용하는 경우가 있다. 예컨대, 음악방송의 경우 원하는 음악을 선택하는 과정과 선택한 음악을 제공받는 과정이 있을 수 있다. 이 때, 음악방송에 연결되는 첫 번째 연결은 주로 제어를 위해서 사용되는 것으로서 정해진 포트번호를 사용하여 상호간 트래픽을 주고있으며, 이는 제1트래픽 유형(21), 제2트래픽 유형(22) 또는 제3트래픽 유형(23)이 된다. 하지만 선택된 음악을 제공받는 두 번째 연결은 상기 제어연결을 통해서 서버-단말간 사용할 포트번호를 교환한 후에 이루어진다. 이 두 번째 연결된 트래픽의 유형을 제4트래픽 유형(24)로 분류하며, 제4트래픽 유형(24)에 해당되는 트래픽은 정해진 포트번호가 없으며, 다만 제어연결에 흐르는 트래픽을 살펴보고 사용될 포트번호를 추출해야만 트래픽을 식별할 수 있게 된다.

<33> 제5트래픽 유형(25)는 이상의 4가지 유형으로 식별되지 않는 응용을 의미하며, 본 발명의 상세 분석대상에서 제외되는 트래픽이다. 통상 일부 사용자들이 임의로 포트번호를 사용하거나 널리 알려지지 않은 응용으로 인해 발생되는 트래픽들이며, 상대적으로 회선에서 점유하는 비율이 작고 응용을 식별하는 작업이 매우 어려운 대상이다.

<34> 이상에서와 같이, 본 발명에서는 트래픽을 5가지 유형으로 나누고 이를 분석함으로써, 효과적으로 트래픽 분석을 할 수 있다.

<35> 도 3은 도 1에 도시된 분석서버(20)에서 수행되는 트래픽 분석 방법의 일실시예를 나타내는 흐름도이다.

<36> 도 1 내지 도 3을 참조하여, 분석서버(20)는 측정장치들(10)로부터 전송된 플로우 정보들을 이용하여 트래픽 유형을 식별하고 통계처리를 수행하게 되는데, 트래픽 유형 식별은 도 2에서 설명된 유형별로 트래픽을 분류하여 응용을 식별하게 된다.

<37> 먼저, 분석서버(20)는 포트 번호만으로 응용식별이 이루어지는 제1트래픽 유형(21)에 대해서 먼저 응용식별을 수행한다(제301단계). 이 때, 분석서버(20)는 제1트래픽 유형에 속한 제4트래픽 유형(24)에 대한 식별자료가 있는가를 확인하여 있으면 이를 추출하여 자료 저장부(230)에 보관한다(제302단계). 도 2를 참조하여 전술된 바와 같이, 제4트래픽 유형(24)의 경우, 제어연결에 흐르는 트래픽을 살펴보고 사용될 포트번호를 추출해야하며, 만약 제301단계에서 식별된 트래픽이 제어연결에 대한 트래픽이라면, 이 트래픽에는 제4트래픽 유형(24)에 대한 식별자료를 포함하고 있으므로 이를 추출하여 보관하며, 향후, 제4트래픽 유형(24) 식별시 이 정보를 이용한다.

<38> 제302단계 후에, 분석서버(20)는 제1트래픽 유형(21)을 식별하고 남은 플로우 정보 중에 제2트래픽 유형(22)을 식별한다(제303단계). 또한, 제2트래픽 유형(22)을 식별하면서 해당 플로우가 제3트래픽 유형(23)의 역방향에 해당되면 제3트래픽 유형의 식별자료를 추출 및 보관한다(제304단계). 또한, 제302단계에서와 마찬가지로 제4트래픽 유형(24)에 대한 식별자료가 있으면 이를 추출 및 보관한다(제305단계).

<39> 전술된 바와 같이, 인터넷의 경우 양방향 트래픽경로가 비대칭이기 때문에 다른 회선에 해당 플로우의 역방향 플로우가 존재할 수 있는데 이를 보다 명확히 분석하기 위해서 여러 지점에서 측정된 자료를 상호 연계하여 분석이 수행되어야 한다. 따라서, 제302단계, 제304단계 및 제305단계에서 식별된 제3트래픽 유형(23) 및 제4트래픽 유형(24)를 다른 회선에서 생성된 것까지 같이 고려함으로써 다지점에서의 트래픽을 상호 연계하여 분석하게 된다. 제3트래픽 유형(23)은 제2트래픽 유형(22)의 역방향 트래픽으로 나타날 수 있는데 이를 위해서 해당 회선에서 생성된 제3트래픽 유형(23) 식별자료뿐만 아니라 다른 지점에서 얻어진 제3트래픽 유형 식별자료를 참조하여 응용식별을 수행한다(제306단계).

<40> 제306단계 후에, 제4트래픽 유형(24)를 식별할 때도 다른 회선의 식별 자료를 참조하여 응용식별을 수행한다(제307단계).

<41> 이상에서, 제1트래픽 유형 내지 제4트래픽 유형의 네가지 유형에 해당되지 않는 트래픽은 제5트래픽 유형(25)로 처리되며, 향후 새로운 응용을 모니터링 하기 위해서 포트 통계량을 계산하는 등의 통계처리하여 저장한다(제308단계). 이처럼, 제5트래픽 유형(25)에 대해 통계처리를 하는 이유는 특별히 분류되지 않은 유형의 트래픽이지만 자주 나타나는 트래픽의 경우 새로운 트래픽 식별 유형으로 분류하거나 또는 제1트래픽 유형(21) 내지 제4트래픽 유형(24)의 범주에 포함시키기 위함이다.

<42> 제308단계 후에, 식별된 트래픽들의 유형은 다시 다양한 보고서 형태로 가공되어 자료 저장부(230)에 저장되며(제309단계), 향후 사용자의 요구에 의해 다양한 형태로 사용자 인터페이스(240)를 통하여 제공된다.

<43> 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플라피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<44> 이상 도면과 명세서에서 최적 실시예들이 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

【발명의 효과】

<45> 상술한 바와 같이, 본 발명에 의한 트래픽 측정 시스템 및 그의 트래픽 분석 방법에 따르면 인터넷망에서 트래픽을 측정하고 이를 가공하여 상세한 응용별 트래픽 통계자료를 생성할 수 있다. 특히, 다지점의 측정자료를 동시에 고려하여 분석하고, IP 패킷의 페이로드에 포함된 응용의 헤더로부터 응용을 식별할 수 있는 자료를 실시간으로 추출함으로써 상세한 트래픽 분석결과를 제공할 수 있다.

【특허청구범위】

【청구항 1】

인터넷 회선에 흐르는 모든 패킷을 수집하고, 수집된 패킷에서 트래픽 분석에 필요한 정보만을 추출하고, 추출된 정보를 소정의 플로우 형태로 가공하는 다수의 측정장치; 및

상기 다수의 측정장치들 각각에서 전달되는 트래픽 정보를 상호연계 분석하여 트래픽의 응용을 식별하고, 식별된 응용을 소정의 트래픽 유형으로 분류하여 그 결과를 출력하는 분석서버를 포함하는 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 2】

제1항에 있어서,

GPS 위성 또는 CDMA 기지국으로부터 시각신호를 추출하여 상기 다수의 측정장치들의 시각이 동일하게 유지되도록 제어하는 다수의 시각수신장치들을 더 포함하는 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 3】

제1항 또는 제2항에 있어서, 상기 다수의 측정장치는

라우터 연결회선으로부터 상기 인터넷 회선에 흐르는 모든 패킷정보를 수집하고 수집된 패킷별로 수집 시각을 기록하는 패킷 수집부;

상기 패킷 수집부에서 수집된 패킷으로부터 목적지 주소, 프로토콜 및 포트번호를 포함하는 정보가 동일한 패킷을 모아 하나의 플로우로서 생성하고, 각 패킷의 내용을 분

석하여 응용별 상세 분석에 필요한 정보를 추출하여 플로우별로 저장하는 플로우 생성부; 및

정해진 시간에 따라 상기 플로우 생성부에 의해 저장된 정보를 상기 분석서버로 전송하는 전송부를 포함하는 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 4】

제3항에 있어서, 상기 패킷 수집부는

태핑, 포트 미러링 또는 신호 분배기 등을 사용하여 필요한 패킷 정보를 수집하는 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 5】

제3항에 있어서, 상기 응용별 상세 분석에 필요한 정보는 패킷의 페이로드에서 응용을 식별할 수 있는 동작관련 정보인 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 6】

제1항 또는 제2항에 있어서, 상기 분석서버는

상기 다수의 측정장치들로부터 전송되는 수집된 패킷정보를 수신하는 데이터 수신부;

상기 데이터 수신부를 통해 상기 다수의 측정장치들로부터 제공되는 정보를 상호 연계하여 응용별 상세 분석하고, 분석 결과에 따라 상기 트래픽 유형으로 분류하는 분석서버;

상기 분석서버의 분석 결과를 저장하는 자료 저장부; 및

상기 자료 저장부에 저장된 트래픽 분석 결과를 사용자가 요구하는 다양한 방식으로 사용자에게 표시하는 사용자 인터페이스를 포함하는 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 7】

제6항에 있어서, 상기 분석서버는

상기 트래픽 분석부(200)에서 분석된 결과를 소정의 보고서 형태로 가공하고, 가공된 보고서를 상기 자료 저장부에 저장하는 보고서 출력부를 더 포함하고,

상기 보고서는 상기 사용자 인터페이스를 통해 사용자에게 표시되는 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 8】

제1항에 있어서, 상기 트래픽 유형은

TCP/UDP 포트번호만으로 응용식별이 가능한 제1트래픽 유형;

패킷의 페이로드에 포함된 응용헤더 및 동작관련 정보를 수집해야 응용식별이 되는 제2트래픽 유형;

상기 제2트래픽 유형의 역방향 트래픽 중에 자체적으로 응용에 관한 정보가 존재하지 않기 때문에 상기 제2트래픽 유형으로부터 응용 정보를 추출해야만 응용식별이 가능한 제3트래픽 유형;

포트번호가 정해져 있지 않으며, 다른 플로우를 통하여 사용할 포트번호가 교환되어 다른 플로우의 내부정보를 바탕으로 응용식별이 가능한 제4트래픽 유형; 및

상기 제1 내지 제4트래픽 유형 중 어느 하나로도 분류되지 않는 제5트래픽 유형을 포함하는 것을 특징으로 하는 트래픽 측정 시스템.

【청구항 9】

인터넷 회선에 흐르는 패킷을 수집하여 트래픽 분석하여 패킷의 응용을 식별하는 트래픽 측정 시스템에서 수행되는 트래픽 분석방법에 있어서,

(a) 소정의 형태로 가공된 플로우 정보로부터 포트 번호만으로 응용식별이 가능한 제1트래픽 유형을 분류하는 단계;

(b)상기 제1트래픽 유형을 식별하고 남은 플로우 정보에서 패킷의 페이로드에 포함된 응용헤더 및 동작관련 정보를 수집해야 응용식별이 가능한 제2트래픽 유형을 분류하는 단계;

(c) 상기 제2트래픽 유형을 식별하고 남은 플로우 정보와 다른 지점에서 측정된 해당 플로우의 역방향 플로우 정보를 상호 연계 분석함으로써 응용식별되는 제3트래픽 유형을 분류하는 단계;

(d)상기 제3트래픽 유형을 식별하고 남은 플로우 정보중 포트번호가 정해져 있지 않아, 다른 지점에서 측정된 플로우 정보를 통하여 응용식별이 가능한 제4트래픽 유형을 분류하는 단계; 및

(e)상기 제4트래픽 유형을 식별하고 남은 플로우 정보를 제5트래픽 유형으로 분류하는 단계를 포함하는 것을 특징으로 하는 트래픽 분석 방법.

【청구항 10】

제9항에 있어서, 상기 (a)단계에서 상기 플로우 정보는

인터넷 회선을 흐르는 패킷에서 동일한 목적지 주소, 동일한 프로토콜 및 동일한 포트번호를 갖는 패킷인 것을 특징으로 하는 트래픽 분석 방법.

【청구항 11】

제9항에 있어서, 상기 (a)단계 후에,

상기 제1트래픽 유형에 속한 트래픽에 상기 제4유형에 대한 식별자료가 있는가를 확인하여 있으면 이를 추출하여 저장하는 단계를 더 포함하는 것을 특징으로 하는 트래픽 분석 방법.

【청구항 12】

제9항에 있어서, 상기 (b)단계 후에,

상기 제2트래픽 유형에 속한 트래픽이 상기 제3트래픽 유형으로 분류되는 트래픽의 역방향 트래픽이라면 제3트래픽 유형으로 분류되는 트래픽의 식별자료를 추출하여 저장하는 단계를 더 포함하는 것을 특징으로 하는 트래픽 분석 방법.

【청구항 13】

제9항에 있어서, 상기 (b)단계 후에,

상기 제2트래픽 유형에 속한 트래픽에 상기 제4유형에 대한 식별자료가 있는가를 확인하여 있으면 이를 추출하여 저장하는 단계를 더 포함하는 것을 특징으로 하는 트래픽 분석 방법.

【청구항 14】

제9항에 있어서, 상기 (e)단계 후에,

상기 제5트래픽 유형으로 분류된 트래픽은 응용을 모니터링 하기 위해서 포트 통계량을 계산과 같은 통계처리를 하고, 통계처리 결과를 저장하는 단계를 더 포함하는 것을 특징으로 하는 트래픽 분석 방법.

【청구항 15】

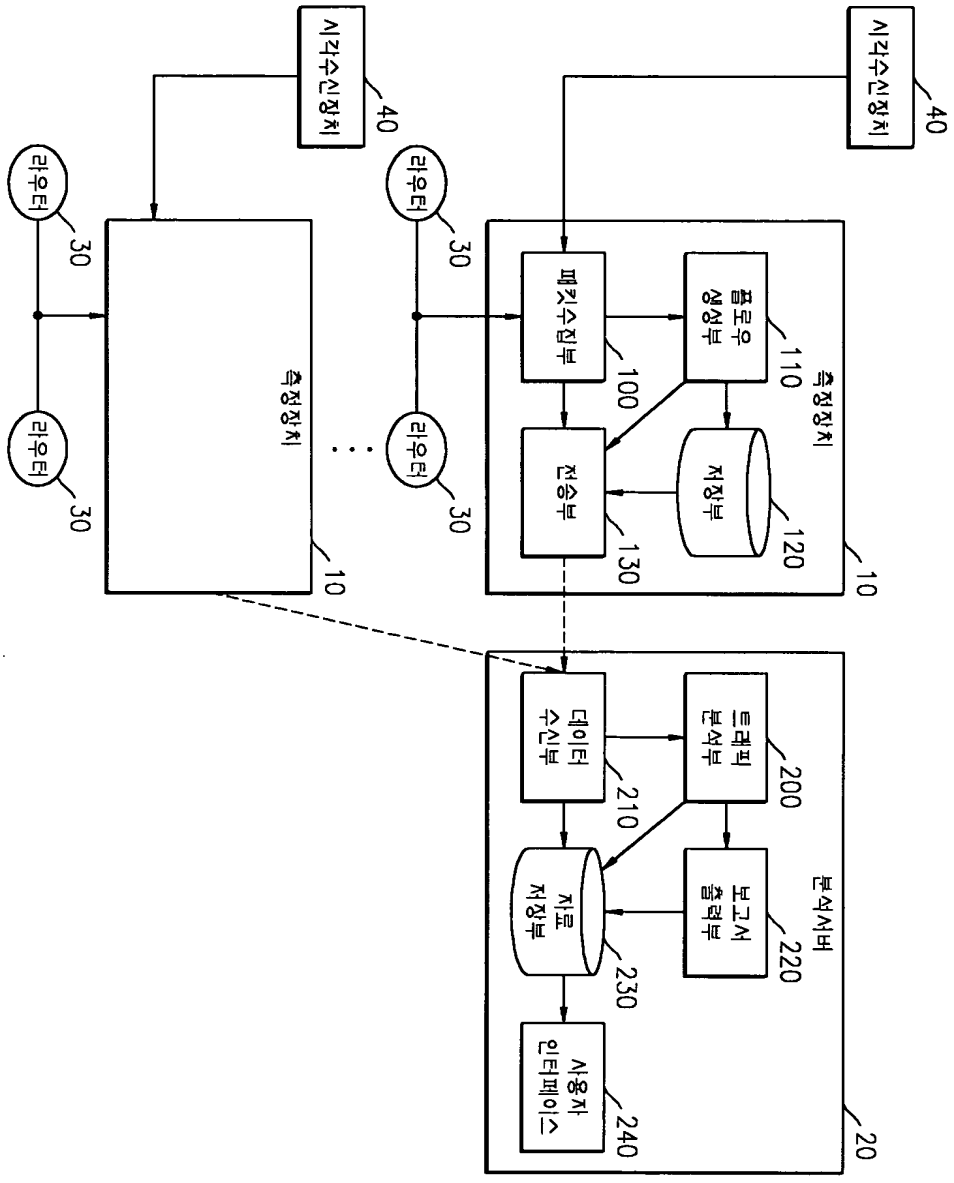
제9항에 있어서, 상기 (e)단계 후에, 식별된 트래픽 유형을 사용자가 요구하는 소정의 보고서 형태로 가공하여 저장하거나 또는 사용자 인터페이스를 통해 제공하는 단계를 더 포함하는 것을 특징으로 하는 트래픽 분석 방법.

【청구항 16】

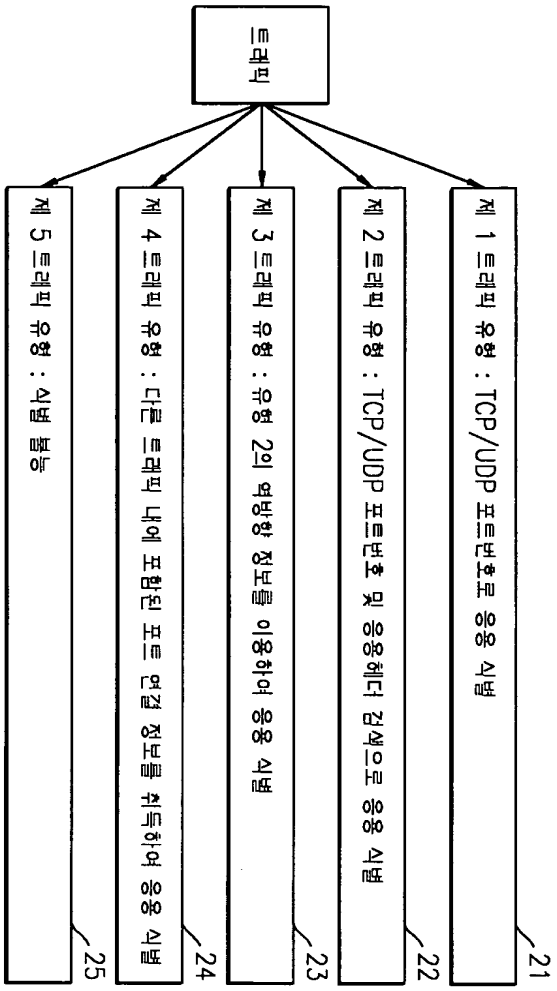
제9항 내지 제15항의 트래픽 분석 방법을 컴퓨터에서 실행 가능한 프로그램 코드로 기록한 기록 매체.

【도면】

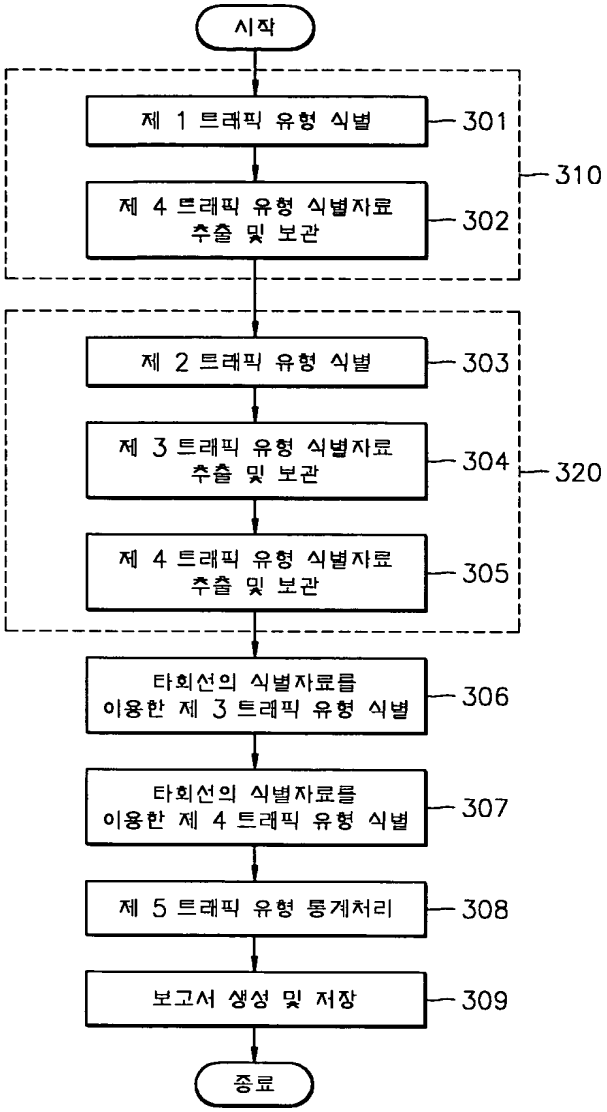
【도 1】


시각수신장치
40
시각수신장치
40
리우터
30
리우터
30
리우터
30
리우터
30
측정장치
10
패킷수집부
100
플로우 생성부
110
전송부
130
저장부
120
측정장치
10
데이터 수신부
210
트래픽 분석부
200
보고서 출력부
220
자료 저장부
230
사용자 인터페이스
240
분석서버
20

【도 2】


트래픽
제 1 트래픽 유형 : TCP/UDP 포트번호로 응용 식별
제 2 트래픽 유형 : TCP/UDP 포트번호 및 응용헤더 검색으로 응용 식별
제 3 트래픽 유형 : 유형 2의 역방향 정보를 이용하여 응용 식별
제 4 트래픽 유형 : 다른 트래픽 내에 포함된 포트 연결 정보를 취득하여 응용 식별
제 5 트래픽 유형 : 식별 불능
21
22
23
24
25

【도 3】


시작
제 1 트래픽 유형 식별
301
제 4 트래픽 유형 식별자료 추출 및 보관
302
310
제 2 트래픽 유형 식별
303
제 3 트래픽 유형 식별자료 추출 및 보관
304
제 4 트래픽 유형 식별자료 추출 및 보관
305
320
타회선의 식별자료를 이용한 제 3 트래픽 유형 식별
306
타회선의 식별자료를 이용한 제 4 트래픽 유형 식별
307
제 5 트래픽 유형 통계처리
308
보고서 생성 및 저장
309
종료